

**AFFIDAVIT OF SPECIAL AGENT BENJAMIN MILLER IN SUPPORT OF  
APPLICATIONS FOR A CRIMINAL COMPLAINT AND A SEARCH WARRANT**

I, Benjamin Miller, having been duly sworn, do hereby depose and state as follows:

**Agent Background**

1. I am a Special Agent with Homeland Security Investigations (“HSI”) and have been so employed since June 2010. I have successfully completed a training program in conducting criminal investigations at the Federal Law Enforcement Training Center in Brunswick, Georgia. In 2007, I graduated from Northeastern University in Boston with a Bachelor of Science degree in Criminal Justice, and in 2010, I received my Master’s degree from Northeastern University in Criminal Justice. My current duties as an HSI Special Agent include conducting investigations involving the fraudulent acquisition, production, and misuse of U.S. immigration documents, U.S. passports, and identity documents. Due to my training, experience, and conversations with other law enforcement officers, I am familiar with the methods, routines, and practices of document counterfeiters, vendors, and persons who fraudulently obtain or assume false identities.

2. I am also a member of HSI’s Document and Benefit Fraud Task Force (“DBFTF”), a specialized field investigative group comprised of personnel from various state, local and federal agencies with expertise in detecting, deterring, and disrupting organizations and individuals involved in various types of document, identity, and benefit fraud schemes.

**Purpose of Affidavit**

3. I submit this affidavit in support of an application for a criminal complaint seeking an arrest warrant for Cristiano RIBEIRO DE MOURA on the charge of 18 U.S.C. § 1028(a)(1), Fraud in Connection with Identification Documents, Authentication Features, and Information.

4. I also submit this affidavit in support of an application for a search warrant for the following property: 153 2nd Street, Apartment 161, Framingham, Massachusetts, as described in Attachment A. I have probable cause to believe that this property contains evidence, fruits, and instrumentalities of the crime identified above, as described in Attachment B.

5. This affidavit is based on my personal knowledge, information provided to me by other law enforcement officers and federal agents, and my review of records described herein. This affidavit is not intended to set forth all of the information that I have learned during this investigation, but includes only the information necessary to establish probable cause for the requested criminal complaint and search warrant.

### **Probable Cause**

#### **Background**

6. On June 25, 2019, an individual later identified as Cristiano RIBEIRO DE MOURA (“RIBEIRO DE MOURA”) was in communication via telephone and the application “WhatsApp” with Confidential Informant #1 (“CI #1”) and Confidential Informant #2 (“CI #2”).<sup>1</sup> The CIs informed DBFTF agents that RIBEIRO DE MOURA offered to produce and sell two counterfeit Lawful Permanent Residence (“LPR”) cards and two counterfeit Social Security Number (“SSN”) cards for the price of \$350 per set (1 LPR and 1 SSN card) to each CI. RIBEIRO DE MOURA told the CIs that he would require a digital photograph of each CI and the biographical information, including the names and dates of birth, they wanted to appear on

---

<sup>1</sup> CI #1 has a criminal history that consists of an arrest for larceny, a charge that was later dismissed. CI #1 is not present in the United States legally. CI #2 was encountered by HSI agents in 2012 and it was determined that CI #2 is not present in the United States legally. Both CIs were placed in deferred action in exchange for their cooperation. Both CIs have cooperated with law enforcement in other cases that have resulted in several arrests. Certain information provided by the CIs has been independently corroborated. Based on this and my personal observations of the CIs, I deem the information they have provided during this investigation to be reliable.

the documents. RIBEIRO DE MOURA used the telephone number 954-232-5960 to communicate with the CIs.

7. At the direction of DBFTF agents, the CIs agreed to purchase two sets of counterfeit documents from RIBEIRO DE MOURA to include a set for CI #1 and one set for CI #2. The CIs were instructed to provide RIBEIRO DE MOURA with digital photographs and to create fake names and dates of birth for this and any future transactions.

#### **The First Document Purchase**

8. On July 2, 2019, CI #1 and CI #2 were given \$700 by the DBFTF to purchase two sets of counterfeit documents from RIBEIRO DE MOURA. Prior to the meeting with ROBEIRO DE MOURA, CI #1 was given a video and audio recording device. While communicating with RIBEIRO DE MOURA via telephone text message and WhatsApp, RIBEIRO DE MOURA told the CIs to meet him at his residence and provided the following address: 153 2nd Street, Framingham, Massachusetts. The CIs relayed this information to DBFTF agents.

9. At approximately 7:00 p.m. that evening, DBFTF agents observed a black Honda Civic bearing Massachusetts license plate 866PM3 approached the CIs, who were standing outside of the building marked "153" on 2nd Street in Framingham, Massachusetts. The DBFTF agents saw the driver of the Honda, RIBEIRO DE MOURA, speak with the CIs while remaining inside of the car. RIBIERO DE MOURA asked the CIs for the money while retrieving the two sets of documents from beneath his leg. This transaction was recorded by CI #1. The CIs informed DBFTF agents that CI #1 handed RIBEIRO DE MOURA \$700 cash in exchange for the documents.

10. A review of the documents purchased from RIBEIRO DE MOURA included two

counterfeit LPR cards, each bearing the photograph of the respective CI and containing the biographical data provided by the CIs, and two Social Security cards. The Social Security cards bore the names provided by the CIs, however the numbers on the cards were provided by RIBEIRO DE MOURA.

### **The Second Document Purchase**

11. On or about July 28, 2019, the CIs were in communication with RIBEIRO DE MOURA via telephone and WhatsApp regarding the purchase of an additional set of counterfeit LPR and SSN for another individual. The CIs relayed the information to DBFTF agents. According to the CIs, RIBEIRO DE MOURA stated that the CIs would have to provide the digital photograph of the individual who would be using the documents as well as that individual's biographical information, namely, his/her name and date of birth. RIBEIRO DE MOURA reaffirmed the price of \$350 for the set and told the CIs to come back to the same location on July 30, 2019, after 7:30 p.m. to pick up the documents.

12. On July 30, 2019, CI #1 was given a video and audio recording device and \$350 by the DBFTF to pay for the counterfeit documents.

13. DBFTF agents set up to surveil the area of 153 2nd Street, Framingham, Massachusetts and observed a male matching the description of RIBEIRO DE MOURA exit the building and enter the same black Honda Civic bearing MA license plate 866PM3. The vehicle departed the parking lot at approximately 7:26 p.m. and returned approximately five minutes later.

14. At approximately 7:30 p.m., DBFTF agents saw the CIs arrive and park in the front parking lot of the building numbered 153 on 2nd Street in Framingham, Massachusetts.

The CIs told RIBEIRO DE MOURA that they were present, which the CIs relayed to the DBFTF agents.

15. DBFTF agents observed RIBEIRO DE MOURA exit the building numbered 153 and sit on the front stoop of the building when the CIs approached. The CIs reported to DBFTF agents that CI #1 gave RIBEIRO DE MOURA \$350 dollars for one counterfeit LPR card and one counterfeit SSN card that RIBEIRO DE MOURA removed from his left side.

16. Upon review, the documents purchased from RIBEIRO DE MOURA included one LPR card bearing the digital photograph, name, and date of birth the CIs provided RIBEIRO DE MOURA. The SSN card bore the name the CIs provided, however RIBEIRO DE MOURA provided the SSN.

#### **The Third Document Purchase and Initial Program Download**

17. The CIs informed DBFTF agents that on or about July 31, 2019, they were in communication with RIBEIRO DE MOURA via telephone and WhatsApp regarding the purchase of another set of counterfeit documents and the computer software that RIBEIRO DE MOURA uses to create them. According to the CIs, RIBEIRO DE MOURA stated he could make an additional set of the counterfeit documents and transfer the software program to the CIs' laptop for the price of \$2,500. RIBEIRO DE MOURA told the CIs that they would need an older model laptop equipped with "Windows 7." RIBEIRO DE MOURA told the CIs that he would show them how to create the counterfeit documents, provide a sample of the paper stock, and show the CIs the type of printer needed.

18. On August 14, 2019, the CIs were provided with a laptop ("laptop") by the DBFTF that had been completely wiped and loaded with Windows 7. The CIs were given \$2,500 by the DBFTF to be used as payment to RIBEIRO DE MOURA for the counterfeit

documents and computer software program. CI #1 also was given an audio and video recording device for the meeting.

19. At approximately 7:18 p.m. on August 14, 2019, DBFTF agents observed the CIs arrive at 153 2nd Street, Framingham, Massachusetts.

20. At approximately 7:40 p.m., the CIs walked around to the stoop on the back side of the building and were met by RIBEIRO DE MOURA. DBFTF agents saw the CIs give the laptop to RIBEIRO DE MOURA. The recording device worn by CI #1 captured RIBEIRO DE MOURA immediately opening the laptop, conducting a review of the computer, and attempting to transfer the software program to the laptop.

21. RIBEIRO DE MOURA told the CIs that he would need some time to create the latest counterfeit LPR and SSN cards, and that the CIs could return in approximately thirty minutes. This interaction was recorded. At approximately 8:18 p.m., DBFTF agents observed the CIs as they allowed RIBEIRO DE MOURA to take the laptop inside the building. The CIs then left.

22. DBFTF debriefed the CIs at this time. The CIs explained that the transfer of the computer program was taking longer than anticipated, but that RIBEIRO DE MOURA stated that he would have the counterfeit documents completed shortly.

23. At approximately 9:04 p.m., DBFTF agents observed as the CIs returned to 153 2nd Street, Framingham, Massachusetts and met with RIBEIRO DE MOURA at the rear stoop of the building. RIBEIRO DE MOURA told the CIs that they needed to purchase a laminator and specific paper from "Staples." This interaction was recorded by the device worn by CI # 1. At approximately 9:31 p.m., RIBEIRO DE MOURA invited the CIs into his apartment. The CIs followed RIBEIRO DE MOURA through the rear door of the building and down the stairs to the

first door on the right, which the CIs reported was identified with the number “161.”

24. While inside the residence, RIBEIRO DE MOURA showed the CIs how to finish the counterfeit documents using the software and provided them with one counterfeit LPR card and one SSN card. The CIs gave RIBEIRO DE MOURA \$200 in exchange for the counterfeit documents. This transaction was recorded by CI #1.

25. RIBEIRO DE MOURA told the CIs that he would need to keep the laptop for a few days to complete the transfer of the computer software program. The CIs left the laptop with RIBEIRO DE MOURA, and agreed to pick up the laptop from RIBEIRO DE MOURA on August 19, 2019. This interaction was recorded by CI #1. The CIs then left the residence and met up with DBFTF agents.

26. Upon review, the documents purchased from ROBEIRO DE MOURA included a counterfeit LPR card bearing the photograph and biographical information provided by the CIs. The SSN card bore the name the CIs provided, however the SSN was provided by RIBEIRO DE MOURA.

### **The Laptop Pick-Up**

27. On August 19, 2019, the CIs informed DBFTF agents that they were in communication with RIBEIRO DE MOURA via telephone and WhatsApp to arrange a time for the CIs to pick up the laptop previously given to RIBEIRO DE MOURA on August 14, 2019. The DBFTF gave CI #1 a video and audio recording device to use for the meeting and \$2,300.

28. At approximately 7:45 p.m., DBFTF agents watched as the CIs arrived at 153 2nd Street, Framingham, Massachusetts and proceeded to the rear stoop of the building to meet RIBEIRO DE MOURA. After a brief conversation outside of the building, RIBEIRO DE MOURA led the CIs inside into apartment 161.

29. While inside that residence, RIBEIRO DE MOURA showed the CIs how to open, create, and print various counterfeit documents, including LPR and SSN cards. RIBEIRO DE MOURA showed the CIs how to drag and drop pictures onto the documents and how to edit the information on the documents. RIBEIRO DE MOURA showed the CIs the specific paper to use when printing the documents and how to laminate and cut the documents. RIBEIRO DE MOURA provided the CIs with a sample piece of paper that he uses to create the counterfeit documents. This interaction was recorded by CI #1.

30. The recording shows that the CIs paid RIBEIRO DE MOURA the remaining money owed for the purchase of the computer software program, \$2,300, and in exchange, the CIs took the laptop from RIBEIRO DE MOURA, exited the apartment, and left the building.

#### **Identification of RIBEIRO DE MOURA**

31. DBFTF agents conducted a law enforcement database search of the residence located at 153 2nd Street, Apartment #161, in Framingham, Massachusetts and discovered one resident listed on the utilities as Cristiano RIBEIRO with a date of birth of xx/xx/1987.<sup>2</sup>

32. A search of the Massachusetts Registry of Motor Vehicles database for the above name and date of birth revealed a commercial driver's license, number xxxxx1265, in the name of Cristiano RIBEIRO.<sup>3</sup> The photograph associated with that license depicts the same individual who sold the CIs the counterfeit documents and the computer software program he uses to create the documents.

33. I know, based on my training and experience, that:

- a. It is common for those who use other persons' identities without authorization

---

<sup>2</sup> The full date of birth is known to the Government, but for security purposes, only the birth year is listed herein.

<sup>3</sup> The full license number is known to the Government, but for security purposes, only the last four digits are listed herein.



to conceal fraudulently obtained identification documents in secure locations within their residence to conceal them from law enforcement authorities and to allow for easy access and use when necessary; and,

- b. It is common for individuals who use fraudulently obtained identification documents to retain those documents for substantial periods of time so that they can continue to use the fraudulently obtained identities as needed.

34. Based on my training and experience, I know that individuals who sell fraudulent identification documents, and in particular multiple sets of such documents, often possess evidence relating to the possession, production, and/or sale of fraudulent identification documents, including but not limited to communications with customers or co-conspirators, document templates, printers, laminators, cutting boards, and fraudulent documents that have been produced but not yet sold to the end user.

35. Also based on my training and experience, I know that individuals who produce identification documents utilize computer equipment, such as laptop computers, to create such documents. I also know that creating these documents using these devices can leave remnants of the user's activities on these devices:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather,

that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media, in particular, computers' internal hard drives, contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.
- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

36. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer

specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

- a. The volume of evidence contained in storage media, such as hard disks, flash drives, CDs, and DVDs, can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.
- b. Technical requirements for analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.


37. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this affidavit is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it on-site or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

### **Conclusion**

38. Based on the foregoing, I have probable cause to believe that on or about July 30, 2019, Cristiano RIBEIRO DE MOURA knowingly produced a false identification document without lawful authority that appears to have been issued by or under the authority of the United States, in violation of 18 U.S.C. § 1028(a)(1).

39. Based on the foregoing, I have probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B, are located in the premises described in Attachment A.

Sworn to under the pains and penalties of perjury.

  
BENJAMIN MILLER  
Special Agent  
Homeland Security Investigations

Subscribed and sworn before me on September 5, 2019

  
HON. M. PAGE KELLEY  
United States Magistrate Judge



**ATTACHMENT A**  
**Premises To Be Searched**

The location to be searched is Apartment 161, 153 2nd Street, Framingham, Massachusetts, a multi-family residence building. The front of the building is marked with the numbers “153.” Apartment 161 is reached by entering through the door located at the rear of the building and proceeding down a set of stairs. Apartment 161 is the first door on the right at the bottom of the stairs and is marked with the numbers “161.”



**ATTACHMENT B**  
**Evidence to Be Searched for and Seized**

Evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1028(a)(1), including but not limited to:

1. The following records, documents, and items:
  - a. Any and all state, United States, and foreign-issued, or apparently United States, state, and foreign-issued, identification documents, work permits, travel documents, notes, statements, and/or receipts that reference same;
  - b. Any and all immigration documents, or apparently issued immigration documents, including but not limited to United States or foreign-issued (or apparently issued) passports and identification cards;
  - c. Any and all documents identifying citizenship, or apparently issued documents identifying citizenship, including but not limited to birth certificates, voter registration cards, cedula, and social security cards.
2. Any and all tools, and receipts of purchase of said tools, used in the creation, production, and distribution of counterfeit identification documents including:
  - a. Computers, laptops, printers, ink cartridges, printer paper, laminators, and cutting boards;
  - b. Any and all electronic media storage devices such as SIM cards, hard drives, USB drives, memory sticks, tablets, external hard drives, etc.; and,
  - c. Cellular telephones, customer contact lists, and ledgers.
3. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant (“the computer equipment”):

- a. evidence of who used, owned, or controlled the computer equipment;
  - b. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the attachment of other computer hardware or storage media;
  - d. evidence of counter-forensic programs and associated data that are designed to eliminate data;
  - e. evidence of when the computer equipment was used;
  - f. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;
  - g. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage; and,
  - h. Records and tangible objects relating to the ownership, occupancy, or use of the premises to be searched (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers).
4. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraphs 1 and 2.
5. Any and all proceeds of the creation, production, and distribution of counterfeit identification documents.



## **DEFINITIONS**

For the purpose of this warrant:

- A. “Computer equipment” means any computer hardware, computer software, mobile phone, storage media, and data.
- B. “Computer hardware” means any electronic device capable of data processing (such as a computer, smartphone, mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. “Computer software” means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- D. “Storage media” means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- E. “Data” means all information stored on storage media of any form in any storage format and for any purpose.
- F. “A record” is any communication, representation, information or data. A

“record” may be comprised of letters, numbers, pictures, sounds or symbols.

### **RETURN OF SEIZED COMPUTER EQUIPMENT**

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy’s authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes